FSPOS

Finansiella Sektorns Privat-Offentliga Samverkan

# IT-strategiska överväganden – Att bygga robust och kostnadseffektiv disaster recovery

2020-03-23

FSPOS Arbetsgrupp Kontinuitetssäkring

# 1 Inledning

Vikten av robusta IT-system för betalningar, tillgång till kontanter, centrala betalningssystemet och värdepappershandel, som av MSB är utpekade som samhällsviktig verksamhet, kan inte nog understrykas. Det svenska samhället har starka beroenden till dessa verksamheter, varför just finansiella tjänster har definierats som en av Sveriges elva samhällsviktiga sektorer[1]. Kraven på ett robust finansiellt system har gjorts tydlig på alla nivåer i samhället. Senast under våren 2019 konstaterade EBA att "*Trust in the reliability of the financial system is crucial for its proper functioning and is a prerequisite if it is to contribute to the economy as a whole. Effective internal governance arrangements are fundamental if institutions individually and the financial system they form as a whole are to operate well.*"[2]

Som alltid när tid och resurser ska allokeras krävs välunderbyggda beslut, vilket är nog så viktigt vid planering, genomförande och uppbyggnad av en robust och återställningsbar IT-verksamhet. I en IT-verksamhet kan antalet beslutsalternativ kopplat till upprättande och uppföljning av IT-kontinuitet och Disaster Recovery (hädanefter förkortat DR i texten) vara många till antalet och komplexa i sin natur. Därför finns ett behov av stödmaterial som hjälper finanssektorns aktörer i arbetet med IT-strategiska överväganden. Ett sådant stödmaterial kan underlätta vid uppbyggnad och design av IT-miljö och val av lämpliga lösningar och tjänster.

## *1.1 Syfte*

Syftet med detta dokument är att exemplifiera konkreta och användbara IT-strategiska överväganden som aktörer inom den finansiella sektorn bör beakta i arbetet med att bygga IT-kontinuitet och utveckla DR-förmåga. Dokumentet syftar framför allt till att fungera som ett stöd i den interna IT-strategiska diskussionen hos en aktör, och kan inte ge exakta svar på samtliga frågeställningar. Svaren förväntas att framarbetas av aktören själv utifrån dess specifika förutsättningar och arbetssätt. Mottagare och användare av innehållet i detta PM är personer som på en strategisk nivå ansvarar för att utveckla IT-kontinuitets- och DR-förmågan hos en aktör inom den finansiella sektorn.

Detta PM tar tydlig utgångspunkt från, samt baseras på *FSPOS Vägledning för kontinuitetshantering*, specifikt *Appendix G – Kontinuitetshantering för outsourcad verksamhet* samt *Appendix H - Självskattningsformulär*. En majoritet av de frågeställningar som tas upp i detta dokument knyter direkt an till självuppskattningsformuläret i *Appendix H* och utgör därvid ett extra stöd vid analys, kravställning, uppföljning och utveckling/avveckling av outsourcing ur ett kontinuitetsperspektiv.

---

[1] *Vägledning för identifiering av samhällsviktig verksamhet, MSB 2019, Sid. 8*
[2] *EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02, Sid. 6*

Som många andra av FSPOS vägledningar och andra publikationer har detta PM genomgående hämtat inspiration från internationella standarder, Solvens II, Basel II/III och Finansinspektionens föreskrifter FFFS 2014:1, FFFS 2014:4 och FFFS 2014:5. Som komplement till detta dokument finns även andra publikationer utgivna som exempelvis berör styrning och kontroll av IT-verksamheten i försäkringsföretag[3].

## 1.2 Metod och avgränsning

Underlaget till detta PM baseras på inventering av öppna källor och intervjuer. Dokumentet behandlar exemplifieringar på frågeställningar och bör därför inte ses som uttömmande i analysen inom varje område. De frågeställningar som analyseras bör beaktas av beslutsfattare på såväl strategisk, taktisk som operativ nivå, även om dokumentet inte närmare går in på operativ nivå. Dokumentet bottnar inte heller fullständigt i flera frågeställningar. Mot slutet av dokumentet tas några övriga överväganden upp som har berörts tidigare men inte utvecklats djupare.

De frågeställningar som behandlas i detta PM syftar till att underlätta vid strategiska och kostnadsdrivande beslut på bolagsnivå för att fastställa riskaptit och investeringsmål för IT-kontinuitet. En avgränsning är dock att dokumentet inte närmare behandlar den eventuella riskaptit och de investeringsmål som ledningen har satt upp på förhand.

## 1.3 Centrala begrepp

Två centrala begrepp som används flitigt i detta PM är *IT-kontinuitet* och *Disaster Recovery (DR)*. Ett IT-strategiskt övervägande kopplat till IT-kontinuitet och DR innebär att frågeställningar som berör till exempel risker, alternativa tillvägagångssätt och strategisk inriktning beaktas. Överväganden kopplat till området IT-kontinuitet innefattar holistiska angreppssätt som berör frågor om uppbyggnad och design av IT-miljön, styrning, förmågor och processer, medan överväganden relaterade till DR berör specifika förmågor i syfte att snabbt kunna återställa kritiska funktioner i verksamheten efter ett haveri.

I detta PM används både begreppen information och informationstillgångar. Enligt MSB[4] finns en skillnad mellan dessa begrepp, där begreppet informationstillgångar tydligare pekar på information som är skyddsvärd. Enbart för att information finns inom en organisation behöver den inte vara en tillgång eller ha ett skyddsvärde. Då merparten av frågeställningarna i detta dokument avser organisationens samtliga informationstillgångar, oberoende skyddsvärde, används begreppet information i första hand.

---

[3] *FI-tillsyn – Styrning och kontroll av IT-verksamheten i försäkringsföretag, Nr 8, 15 november 2018*
[4] *Terminologi och begrepp inom informationssäkerhet, MSB 2016, Sid. 14*

# 2 IT-strategiska överväganden

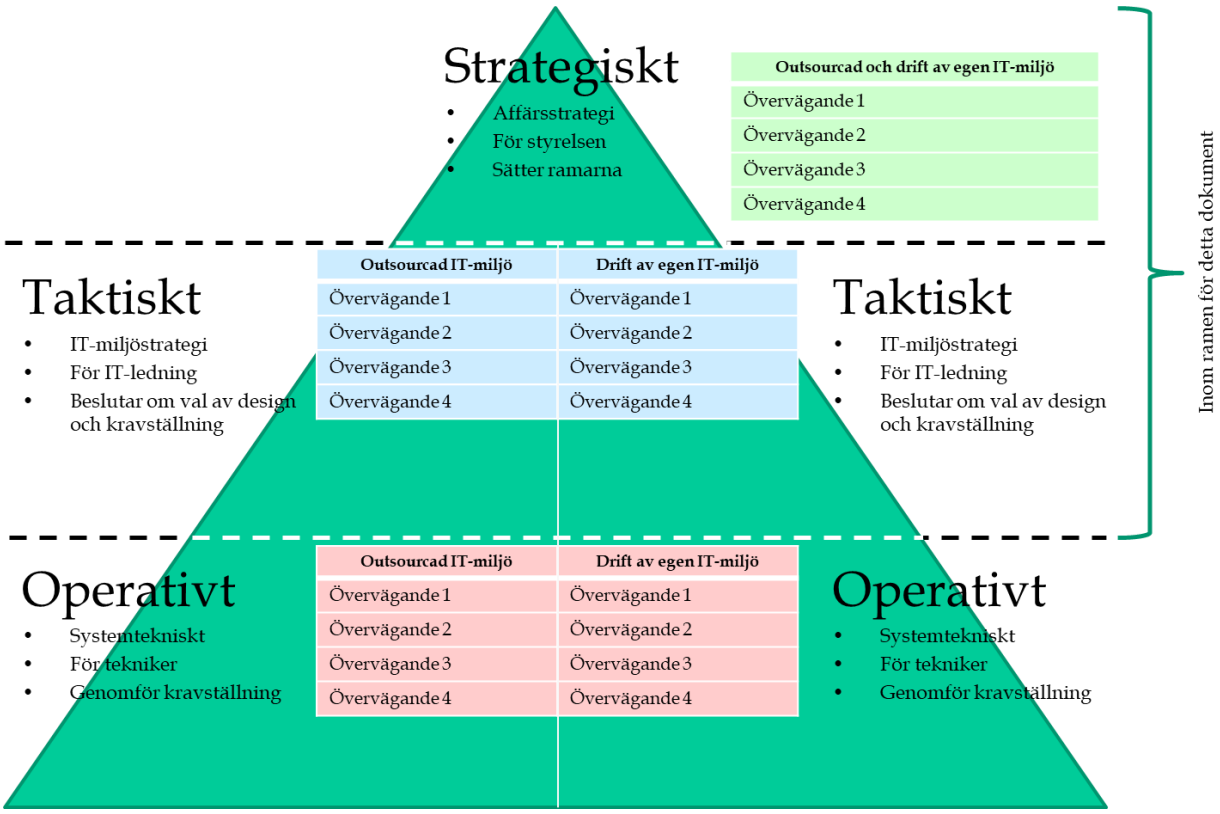
Centrala IT-strategiska överväganden som analyseras i detta PM är:

- *Hur ska information hanteras utifrån hur den har klassificerats enligt organisationens beslutade kriteriemodell?*
- *Hur säkerställs, genom styrning och kontroll, att information hanteras korrekt enligt hur den har klassificerats?*
- *Hur utvecklas och verifieras förmågan att skydda information genom övning och test?*

Dessa presenteras i separata avsnitt i dokumentet. För varje centralt övervägande beskrivs en bakgrund; här beskrivs bland annat syfte, mål och kontext, det vill säga varför just detta övervägande är viktigt att beakta. Kopplat till vardera av dessa tre centrala IT-strategiska överväganden finns ett antal underliggande och mer konkreta strategiska och taktiska överväganden som anges i punktform och beskrivs i löpande text. Det finns ingen inbördes rangordning mellan underliggande överväganden.

Genom väl underbyggda och analyserande frågeställningar exemplifieras tre centrala IT-strategiska överväganden för den finansiella sektorn på ett konkret och användbart sätt. Dessa exempel på frågeställningar bör ge aktörer och sektorn i stort ett lämpligt stöd vid beslut om uppbyggnad och design av IT-miljö, samt vid val av lämpliga lösningar och tjänster för upprättande och uppföljning av IT-kontinuitet och DR. Olika överväganden skiljer sig dock åt mellan organisationer som driftar sin egen IT-miljö och organisationer som har valt att outsourca den, vilket noga understryks i detta PM. Hos många aktörer finns även en blandad IT-miljö, dvs i egen regi och genom uppdragsavtal för drift, vilket gör dessa frågeställningar än mer komplexa.

I figur 1 nedan illustreras hur IT-strategiska överväganden på ett schematiskt sätt kan tillämpas på strategisk, taktisk och operativ nivå. Denna modell kan vara till nytta för beslutsfattare på respektive nivå. I Bilaga A finns samtliga centrala och underliggande strategiska och taktiska överväganden samlade i en matris för att ge en överskådlig bild av vad som bör beaktas per område.




*Figur 1. Modell för IT-strategiska överväganden på strategisk, taktisk och operativ nivå.*

## 2.1 *Hur ska information hanteras utifrån hur den har klassificerats enligt organisationens beslutade kriteriemodell?*

### Bakgrund

Det är av stor vikt att en aktör inom den finansiella sektorn identifierar och klassificerar sina informationstillgångar med stöd av en beslutad kriteriemodell. Detta IT-strategiska övervägande beaktar hur information i allmänhet bör hanteras, mot bakgrund av klassificeringen. En klassisk kriteriemodell som används för klassificering av information tar hänsyn till standarder och regelverk som till exempel ISO 27001, GDPR[5] och PCI DSS[6] och beaktar verksamhetens risker relaterade till konfidentialitet, riktighet, tillgänglighet, och ibland även spårbarhet. Information klassificeras utifrån ett flertal kriterier. De kriterier som tas upp i ISO 27001 är värde, legala krav, känslighet och betydelse för organisationens verksamhet. Även andra kriterier kan vara relevanta för den egna organisationen. MSB har tagit fram ett metodstöd för systematiskt informationssäkerhetsarbete[7] som ger stöd med arbetet att både skapa och använda en organisationsgemensam kriteriemodell för klassificering av informationstillgångar. Klassificeringen styr i sin tur bland annat konkreta frågeställningar som prioritering av IT-system och tjänster vid återställning, informationssäkerhetskrav, lämpliga skyddsnivåer, etc.

Detta IT-strategiska övervägande fokuserar på frågeställningar relaterade till IT-kontinuitet, det vill säga frågor om uppbyggnad och design av IT-miljö, styrning, förmågor och processer. Typexempel på sådana tekniska IT-kontinuitetsrelaterade frågor är val av intern eller outsourcad drift av IT-miljö samt design av IT-miljö med avseende på förmågan att bevara och skydda information, eller så kallad *continuity by design*. ITIL 4 understryker vikten av att överväga IT-kontinuitet så tidigt som möjligt i designen av IT-system och tjänster då processen för *IT Service Continuity Management* ingår redan i designfasen av livscykelhanteringen.

### Underliggande IT-strategiska överväganden

***Strategisk nivå - Affärsstrategiska beslut för styrelsen eller ledningen som sätter ramarna***

Underliggande IT-strategiska överväganden som analyseras i detta avsnitt är:

[5] *GDPR - General Data Protection Regulation, Dataskyddsförordningen på svenska.*
[6] *PCI DSS - Payment Card Industry Data Security Standard.*
[7] *www.informationssakerhet.se/metodstodet/utforma/#klassningsmodell*

- *Kan information helt, delvis eller inte alls lagras i outsourcad IT-miljö?*
- *Kan information helt, delvis eller inte alls lagras i molnet?*
- *Finns någon information som måste lagras i egen IT-miljö?*
- *Finns tillräcklig kompetens internt för att drifta egen IT-miljö?*
- *Hur förhåller sig organisationens riskaptit till val av sourcing?*
- *Är det möjligt att lagra information utanför Sveriges gränser?*
- *Vad blir konsekvenserna av att lagra information utanför Sveriges gränser?*

Varje organisation har olika förutsättningar och måste således förhålla sig till dessa. Ett tidigt strategiskt övervägande som påverkar flera andra beslut är övervägandet om intern eller outsourcad drift av IT-miljö samt inställningen till att lagra information i molnet. En viktig aspekt som kan påverka detta val är organisationens förmåga till intern drift, det vill säga om den information som ska hanteras kan driftas internt med den kompetens och de resurser som finns till förfogande internt, eller inte. Fallet kan vara så att vissa informationstillgångar kräver IT-tekniska lösningar som den egna organisationen saknar förmåga att bygga själv, eller robusta IT-miljöer som organisationen inte kan bekosta själv. En nackdel med outsourcing kan vara försämrade möjligheter till styrning och kontroll. Därför bör fördelar och nackdelar noga analyseras gentemot organisationens krav och förutsättningar inför beslut om intern eller outsourcad drift av IT-miljö.

Information som enligt kriteriemodellen har klassificerats på ett sätt som ställer höga krav på tillgänglighet behöver ibland outsourcas för att upprätthålla uppsatta tillgänglighetskrav. Man bör även ta med i sin bedömning huruvida klassificering av information leder till höga krav på konfidentialitet och därigenom inte kan outsourcas och lagras i specifika länder på grund av risken för spridning. Dessa överväganden, tillsammans med många andra överväganden, är exempel på komplexa frågeställningar som den upphandlande organisationen inte alltid kan analysera på egen hand. En stark rekommendation är därför att alltid, när så är möjligt, ta hjälp av nuvarande leverantörer – eller tilltänkta leverantörer under upphandlingsprocessen – i arbetet med att hitta lämpliga lösningar och tjänster som uppfyller kraven för att bevara informationens skyddsvärden. Under intervjuer med leverantörer av IT-tjänster har det framkommit att de ser en stor fördel i att bli involverade så tidigt som möjligt under upphandlingsprocessen för att säkerställa kravställningarna.

På en strategisk nivå bör organisationen således först analysera förmågan till egen drift samt för- och nackdelar med intern drift kontra outsourcad drift. Utifrån kriteriemodellens utformning och dess påverkan på klassificering av information bör dessa för- och nackdelar, samt risker med lagring av information (helt eller delvis) i molnet, ligga till grund för strategisk design av IT-miljön. Viktigt är också att beakta kravställningar som implicerar att viss information måste lagras i egen IT-miljö av strategiska, lagmässiga eller andra verksamhetsspecifika skäl. Information som utgör en stor verksamhetsrisk vid förlust eller innehåller särskilt känsliga uppgifter bör

analyseras extra noga för att säkerställa att skyddskraven kan upprätthållas under alla omständigheter. MSB har givit ut en vägledning[8] som stöd för att den fysiska informationssäkerheten i förvaring och användning av IT-utrustningar ska motsvara de krav på skydd som respektive organisation har.

Baserat på utkomsten av IT-strategiska överväganden gällande intern eller outsourcad drift av IT-miljö är det viktigt att risker kopplat till olika designval tas i beaktande. Design av robusta IT-system och tjänster handlar bland annat om val av återställningsmetod (cold site, warm site, hot site, etc.), tekniker för feltolerans (spegling, replikering, redundans, etc.), och digitala verktyg för exempelvis backuptagning och återställning. Dessa designval är i allra högsta grad kostnadsdrivande och kan i slutändan påverka beslut om sourcing eller ej. Exempelvis kan en organisation som driftar sin egen IT-miljö sakna ekonomiska medel för en adekvat backup- och återställningshantering.

Oavsett designval eller om information ska lagras i molnet, internt eller outsourcat hos leverantör, bör risker kopplat till varje alternativ noga övervägas. Risker att överväga är kopplat till områden som exempelvis lagkrav, regleringar, policys, tillgänglighetskrav och rykte. Även risker kopplade till underleverantörer av outsourcad drift, det vill säga underleverantörer till den sourcingpartner som man har valt, bör noga beaktas. Långa leverantörskedjor ökar risken för minskad insyn och tillgänglighet i leverantörens verksamhet och öppnar samtidigt upp för andra sårbarheter i tjänsten. Alla dessa parametrar bör beaktas utifrån hur informationen har klassificerats. Riskhanteringen påverkas dels av den faktiska riskanalysen, dels av organisationens riskaptit. Frågan om riskaptit är särskilt viktig vid lagring och hantering av information då den tydligt styr risktagande och beslut vid val av sourcing. Just detta faktum sätter ramarna för det taktiska arbetet.

En särskilt viktig fråga kopplat till detta är lagring av information utanför Sveriges gränser utifrån ett informationssäkerhets- och compliance-perspektiv. När information som innehåller personuppgifter lagras utanför Sverige i annat EU-land gäller samma skydd för personuppgifterna som i Sverige enligt GDPR. Information kan alltså fritt överföras mellan EU-länder utan begränsningar. Överföring av personuppgifter till land utanför EU, så kallad tredjelandsöverföring, medför dock särskilda regler som måste beaktas, till exempel huruvida det finns beslut från EU-kommissionen om att landet har adekvat skyddsnivå eller att relevanta skyddsåtgärder är reglerade i avtal. Finansiella aktörer som har information lagrade i Storbritannien behöver särskilt följa Brexit-processen. Om utträdet sker utan avtal om övergångsbestämmelser för handeln mellan Storbritannien och EU, finns risken att Storbritannien blir ett så kallat tredje land enligt definitionen i GDPR. Säkerhetsskyddslagen tar sikte på säkerhetsskyddsklassificerade uppgifter, men lagen har inga bestämmelser som hindrar finansiella aktörer att lagra dessa utanför Sveriges gränser. Aktören behöver dock se till att uppgifterna skyddas genom en säkerhetsskyddad upphandling med

[8] *Vägledning för fysisk informationssäkerhet i IT-utrymmen, MSB 2013.*

säkerhetsskyddsavtal (SUA). På Finansinspektionens hemsida presenteras nyheter inom ramen för Brexit-processen som påverkar den finansiella sektorn.

***Taktisk nivå - IT-miljöstrategiska beslut för IT-ledning som beslutar om val av design, kravställning och förmågor***

Underliggande IT-strategiska överväganden som analyseras i detta avsnitt är:

- *Hur påverkar kostnaden val av design?*
- *Hur ska organisationen arbeta vid val av sourcing, IT-arkitektur och drift?*
- *Vilka designval är tillämpliga vid outsourcad respektive insourcad IT-miljö?*
- *Vilka riktlinjer för lagring av information i molnet bör tillämpas?*
- *Hur ska information lagras för säker backuphantering?*
- *Hur många datahallar krävs och hur ska information fördelas mellan dem?*
- *Hur ska datahallar rent geografiskt placeras? Vilka krav finns?*

Likt antagandet att varje organisation har en fördefinierad kriteriemodell antas att alla aktörer inom den finansiella sektorn har definierat sin riskaptit på strategisk nivå. Inom ramen för detta IT-strategiska övervägande på taktisk nivå blir frågan således vilka risker som kan accepteras kopplat till olika sourcingalternativ med utgångspunkt från organisationens definierade riskaptit. Varje organisation bör således väga risken med olika sourcingalternativ mot fastställd riskaptit. Då kostnaden alltid är en viktig och drivande faktor för beslut av riskåtgärder bör frågan ställas hur detta påverkar organisationens förmåga till redundans och återställning. Detta är något som måste hanteras på taktisk nivå och drivas inom ramen för kontinuitetsarbetet.

Oberoende av intern eller outsourcad IT-drift bör ytterligare ett antal överväganden beaktas utifrån klassificeringen av informationen. IT-miljörelaterade överväganden bör beaktas vid implementering i syfte att uppfylla de krav på hantering och informationssäkerhetskrav som styrs av klassificeringen. Givet den komplexitet som föreligger vid flytt från insourcad till outsourcad drift, eller vid byte av driftsleverantör, bör risker relaterade till dessa typer av åtgärder noga övervägas, särskilt då dessa åtgärder är tids- och kostnadskrävande att genomföra. Även under själva transformationsprocessen vid flytt av datahall är det viktigt att upprätthålla kontinuiteten. Därför bör risker kopplat till transformationsprocessen hanteras så att informationssäkerhetskraven kan upprätthållas under hela processen.

Överväganden på taktisk nivå berör till stor del samtliga informationstillgångar och till viss del enskilda informationstillgångar, det vill säga vissa beslut påverkar IT-kontinuiteten för enskild information medan andra beslut påverkar all information. Beslut på taktisk nivå påverkar således organisationens lägsta såväl som högsta nivå gällande teknisk redundans och risken för, samt förmåga till, återhämtning av datahallshaveri. Tack vare den klassificering av information som har gjorts kan organisationen anpassa designval för exempelvis tillgänglighet efter kravbild per informationstillgång. Kritiska informationstillgångar med höga tillgänglighetskrav medför ofta höga kostnader för olika tekniska lösningar. Dessa tekniska lösningar kan

i vissa fall även utnyttjas av andra informationstillgångar med lägre tillgänglighetskrav, och i vissa andra fall inte. Viktigt är att också överväga lägsta acceptabla nivå för återställningsbarhet i förhållande till kravställningen för att kunna anpassa datahallens infrastruktur efter det.

Vid lagring av information i molnet finns många viktiga överväganden att beakta på taktisk nivå, och som kommer att vara avgörande för design av IT-miljön. Några exempel på sådana överväganden är val av tjänster som kan läggas ut i molnet, val av molntjänst som sådan (IaaS[9], PaaS[10], SaaS[11]), val av molntjänstleverantör, fördelning av information mellan länder, hantering av risker kopplade till lagring av information i molnet, vilka informationssäkerhetskrav som aktören ska ha på molntjänstleverantören, hur informationssäkerhetskrav som formulerats i avtalsförhållandet följs upp, samt hur molntjänstleverantörer bemöter informationssäkerhetskraven[12]. Gemensamt för alla dessa överväganden är att de kommer att få avgörande betydelse för organisationens personal, arbetssätt för styrning och kontroll, samt möjligheter att testa och verifiera förmågor. Det är inte ovanligt att flera olika typer av molntjänster, samt även flera olika molntjänstleverantörer, behöver nyttjas samtidigt inom organisationen, vilket ökar komplexiteten ytterligare.

För organisationer som lagrar information i datahallar, där driften hanteras antingen i egen regi eller av leverantörer, finns många ytterligare överväganden att beakta då informationen kan lagras på många olika sätt. Information kan lagras på olika media (exempelvis lagring på disk eller lagring på tape) och ha olika geografisk placering (exempelvis lagring in-house eller lagring i molnet). Avgörande är hur ofta man vill få tillgång till informationen, samt hur fort man vill få tillgång till informationen. Tekniker att beakta för säker informationslagring och backuphantering nu och i framtiden är *distributed computing*, *grid computing* och *cloud computing*. En backupstrategi, som är mycket användbar och kan tillämpas av de flesta organisationer, är den så kallade 3-2-1-regeln för backup[13] som anger att man bör behålla tre kopior av sin information, lagrade på två typer av media, med en kopia på annan plats. Genom att tillämpa denna strategi minskar sannolikheten avsevärt att all information går förlorad vid ett större haveri.

Även antal datahallar, fördelningen av information mellan datahallar och geografisk placering är viktiga faktorer som får avgörande betydelse för organisationens förmåga att hantera incidenter och avbrott. Som upphandlande organisation vid outsourcing av datahallar och infrastruktur är det viktigt att känna till vilka krav som ska ställas gentemot leverantör. Organisationer med höga krav på svarstid och tillgänglighet är

---

[9] *IaaS – Infrastructure as a Service*
[10] *PaaS – Platform as a Service*
[11] *SaaS – Software as a Service*
[12] *Säkerhet vid molnlösningar, MSB 2018.*
[13] *The DAM Book: Digital Asset Management for Photographers, Peter Krogh 2005*

ofta medvetna om detta och tar hjälp av leverantörer under upphandlingsprocessen. Några exempel på viktiga kravställningar som aktörer behöver ställa är krav på hur driften sker (det räcker inte med att ställa krav på datahallens design), krav på att datahallarna erbjuder maximal tillgänglighet och säker anslutning till molnet, samt krav på att datahallarnas geografiska placering är rätt för att klara av snabba svarstider. Ytterligare förslag på kravställningar återfinns i *Vägledning för fysisk informationssäkerhet i IT-utrymmen* utgiven av MSB. Det finns även internationella standarder som specificerar olika tillgänglighetsnivåer för datahallar som med fördel kan tillämpas vid outsourcing, exempelvis BICSI, ANSI/TIA-942 och Uptime Institute.

Vid köp av vissa molntjänster, särskilt PaaS och SaaS, kan specifika kravställningar inte alltid ställas explicit gentemot molntjänstleverantören då de bakomliggande tekniska lösningarna ofta är inbakade som en del i tjänsten och är antingen kända (i bästa fall) eller okända (i sämsta fall) för beställaren. Det är därför av största vikt att organisationen skaffar sig all nödvändig kompetens som gör det möjligt att tolka tjänstebeskrivningar och kravställa vid köp av PaaS- och SaaS-tjänster. I studien *Säkerhet vid molnlösningar*, utgiven av MSB, samlas viktiga erfarenheter från offentliga aktörer genom deras upplevda utmaningar i att upphandla molntjänster och höga kravställningar gällande informationssäkerhet. Dessa erfarenheter berör i allra högsta grad även aktörer inom den finansiella sektorn.

## 2.2 *Hur säkerställs, genom styrning och kontroll, att information hanteras korrekt enligt hur den har klassificerats?*

### Bakgrund

Oavsett intern eller outsourcad drift av IT-miljö måste rutiner för styrning och kontroll fastställas, implementeras och efterlevas. Mer fokus på kvalitativ styrning och kontroll, det vill säga uppföljning av faktiska aktiviteter, skapar bättre förutsättningar för organisationens förmåga att efterleva krav än enbart en kvantitativ styrning och kontroll, som i högre utsträckning följer upp mätvärden i sifferform som exempelvis *mål för återställningstid*[14] och *mål för återhämtningspunkt*[15]. En kvalitativ styrning som kontrollerar faktiska aktiviteter ställer högre krav på processförståelse och personliga relationer än en kvantitativ styrning som enbart ställer krav på mätbara siffror. Båda alternativen är således förknippade med såväl för- som nackdelar.

Detta strategiska övervägande fokuserar på frågeställningar relaterade till styrning, kontroll, förmågor, ansvar, processer och rutiner i avseende på IT-kontinuitet och DR.

### Underliggande IT-strategiska överväganden

***Strategisk nivå - Affärsstrategiska beslut för styrelsen eller ledningen som sätter ramarna***

Underliggande IT-strategiska överväganden som analyseras i detta avsnitt är:

- *Hur prioriterat är systemtillgänglighet?*
- *I vilken utsträckning, och hur bör IT-kontinuitet och DR beaktas vid due diligence och författande av outsourcingavtal?*
- *Vad är ambitionsnivån och syftet med styrning och kontroll?*
- *Ska den huvudsakliga DR-förmågan byggas genom köpta tjänster eller interna processer och system?*
- *Bör DR-förmågan kvalificeras genom certifiering och i sådana fall mot vilken standard?*
- *Vilka lagar ska en leverantör följa om leverantören inte är registrerad i Sverige?*

Möjligheten samt behovet av styrning och kontroll beror mycket på hur arbetet är organiserat och vem som ansvarar för vad. En viktig faktor som i allra högsta grad påverkar förmågan till styrning och kontroll är huruvida IT-miljön driftas internt eller om den är outsourcad. Utifrån denna faktor behöver ytterligare aspekter beaktas i arbetet. Vid beslut om outsourcing är avtalsfrågan ett särskilt viktigt område att beakta och analysera närmare. När beslut om outsourcing har tagits bör en särskilt tillsatt organisation göra noggranna överväganden kring hur prioriterat IT-kontinuitet och DR är – en viktig frågeställning som en aktör inom den finansiella sektorn bör kunna besvara baserat på sitt nuvarande kontinuitetsarbete. Detta övervägande bör göras innan avtalsförhandlingar påbörjas med leverantörer. En organisation som genom

[14] *RTO - Recovery Time Objective (ISO 22301).*
[15] *RPO - Recovery Point Objective (ISO 22301).*

konsekvensanalys och riskbedömning har fastställt krav på korta återställningstider för IT-system bör per definition även ha höga tillgänglighetskrav, varför denna fråga bör anses vara prioriterad. Därför är frågan om systemtillgänglighet särskilt viktig att begrunda inför avtalsförhandlingar då svaret på frågan påverkar den prioritet som IT-kontinuitet och DR får i leverantörsavtalet och därigenom kostnaden.

Ambitionsnivån för den interna och externa styrningen och kontrollen påverkar många relaterade beslut, varför det är viktigt att detta fastställs så tidigt som möjligt i avtalsprocessen. Fastställande av systemtillgänglighet och prioritering, inkludering av IT-kontinuitet och DR-hantering vid due diligence[16], författandet av leverantörsavtal vid outsourcing, samt organisationens ambitioner i frågan blir sammantaget ett omfattande arbete som påverkar valet av kontrollfrågor, kontrollfrekvens och upplägg för kontrollarbetet. Här är det särskilt viktigt att styrning och kontroll beaktas och genomförs på samtliga nivåer inom organisationen, det vill säga på strategisk, taktisk och operativ nivå, och att detta hanteras inom ramen för leverantörsavtalet.

Vid due diligence och författande av outsourcingavtal är det ofta fördelaktigt att använda leverantörens *IT Service Continuity Plan (ITSCP)* om underlag. ITSCP är ett begrepp som inte används så mycket i Sverige men desto mer i Europa och USA. ENISA har tagit fram ett förslag[17] om upprättande av ITSCP för sourcad IT-kontinuitet och DR, det vill säga ett samlingsdokument som beskriver var i återställningsprocessen kunden befinner sig vid ett haveri eller en kris i IT-leveransen från leverantören. En ITSCP binder samman all kontinuitetsrelaterad information som exempelvis återgångskapacitet under givna faser i återställningsprocessen och *Service Level Agreement (SLA)* för leverantörens olika DR-miljöer och relaterade förmågor. Denna typ av information är av största värde vid due diligence. Även *EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)* och *EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)* är mycket användbara vid due diligence och författande av outsourcingavtal.

I ett scenario där driften av IT-miljön är outsourcad och möjligheten till att köpa DR-tjänster från en leverantör är aktuell bör organisationen överväga vilka tjänster och förmågor som kan överlämnas till en extern part och vilka som bör behållas internt. Just möjligheten till styrning och kontroll är en viktig faktor att beakta vid köp av externa DR-tjänster. Det finns både för- och nackdelar med att köpa DR-tjänster av en leverantör. En fördel kan vara att den totala kostnaden för DR-hantering minskar genom användning av standardiserade DR-tjänster som exempelvis DRaaS[18] eller inbyggd redundans i den levererade plattformen hos leverantören. En nackdel kan vara den försämrade möjligheten till styrning och kontroll av organisationens DR-

[16] *Företagsbesiktning av den bäst lämpade leverantören - en förutsättning för att gå vidare i dialog om avtalsskrivning.*

[17] *www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-plan/it-service-continuity-plan*

[18] *DRaaS - Disaster Recovery as a Service.*

förmåga i samband med outsourcing av DR-tjänster. Lösningar köpta av en leverantör är ofta svårkontrollerade varför insikten om den faktiska DR-förmågan är svårdefinierad, samtidigt som det kan antas att leverantören som hanterar avbrott i sin vardag är bättre på denna hantering än intern personal som gör det mindre frekvent.

För konkretiserad och förenklad styrning och kontroll kan organisationen ta beslut om att följa särskilda ramverk eller standarder samt kravställa på certifiering i enlighet med sådana. Om organisationen väljer att arbeta efter samma ramverk eller standard som leverantören blir processerna förenliga vilket underlättar förståelsen för kravbilden och kommunikationen mellan beställare och leverantör. Utifrån de tillgängliga alternativen för ramverk och standarder som finns att tillgå, exempelvis ITIL 4, COBIT 2019, ISO 9001, ISO 14001, ISO 27001, ISO 22301, ISO 27031, med flera, bör organisationen väga för- och nackdelar gentemot samtliga standarder och besluta vilka som är mest förenliga med övriga interna processer och arbetssätt. Baserat på ambitionsnivå och externa krav bör även frågan om certifieringskrav på den egna organisationen beaktas. Lägg dock märke till att oavsett certifiering av leverantör äger den upphandlande organisationen alltid ansvaret för styrning och kontroll då finanssektorn är en hårt reglerad bransch, med andra ord kan ansvaret hos aktören för styrning och kontroll aldrig outsourcas.

Baserat på beslut om lagring av information utanför Sveriges gränser bör reglerande lagkrav tydligt definieras som underlag för styrning och kontroll. Utifrån de lagkrav och regleringar som ställer krav på var information ska lagras, är det således viktigt att i ett tidigt stadium tydligt fastställa hur information ska hanteras av en leverantör. Att såväl internt som externt förtydliga dessa lagkravsrelaterade förväntningar är avgörande för ett framgångsrikt samarbete mellan aktör och leverantör. Aktörer som lagrar information hos leverantörer som lyder under amerikansk lagstiftning behöver särskilt uppmärksamma de krav som Cloud Act ställer på molnleverantören[19]. Enligt Cloud Act har amerikanska myndigheter rätt att vid misstanke om grovt brott begära ut information från molnleverantören oavsett vilket land den är etablerad i. En ytterligare konsekvens av att lagra information utanför Sveriges gränser, särskilt utanför Europa, är att möjligheten till att lagföra och driva tvist minskar avsevärt. En riskbedömning behöver göras om organisationen överväger att lagra information hos en leverantör i ett land utanför Sveriges gränser, eller hos en utländsk leverantör etablerad i Sverige med avseende på nationell lagstiftning. Oavsett vilket land det handlar om behöver aktören uppmärksamma de nationella lagar som reglerar informationsbehandling i eller för det aktuella landet.

***Taktisk nivå - IT-miljöstrategiska beslut för IT-ledning som beslutar om val av design, kravställning och förmågor***

Underliggande IT-strategiska överväganden som analyseras i detta avsnitt är:

[19] *Cloud Act – the Clarifying Lawful Overseas Use of Data Act*

- *Vad är budget vid outsourcad IT-miljö och vad ska täckas in?*
- *Ska uppföljning fokusera på kvalitativ eller kvantitativ information?*
- *Vilka DR-förmågor kan överlåtas till leverantör och vilka måste alltid finnas internt?*
- *I vilken omfattning får en eventuell leverantör anlita underleverantörer?*
- *Hur ska IT-kontinuitets- och DR-arbetet följas upp för att säkerställa önskad effekt?*
- *Hur kan leverantörer involveras vid lärandet och förbättringsåtgärder efter inträffade haverier?*
- *Hur säkerställs att informationens skyddsvärden bibehålls under hela DR-processen?*

Innan faktiska krav kan fastställas gentemot en leverantör av drifts- och DR-tjänster bör aktiviteter som ska rymmas inom budgeten definieras och förtydligas. I de fall en eller flera drifts- och DR-tjänster har outsourcats till en leverantör bör organisationen noga överväga och tydligt kommunicera finansieringen av dessa. Monetära[20] såväl som icke-monetära[21] kostnader för outsourcing bör vägas mot samma premisser som vid intern uppbyggnad av sådan förmåga. Exempelvis kan eskaleringskedjor påverkas vilket leder till ökad komplexitet och därigenom ökade icke-monetära kostnader vid outsourcing av exempelvis SOC[22], service desk och andra driftsrelaterade tjänster. Givet dessa och andra kostnadsrelaterade överväganden bör organisationen avgöra vilka drifts- och DR-tjänster som bör behållas internt samt vilka som kan outsourcas.

Beroende på vem som driftar IT-miljön efter att ambitionsnivå och syfte har fastställts bör ytterligare överväganden beaktas. Ett övervägande som tydligt påverkas av ambitionsnivån är vad som ska styras och kontrolleras inom ramen för IT-kontinuitet och DR. Den ambitiösa organisationen konkretiserar kvalitativa aktiviteter[23] att följa upp, medan den mindre ambitiösa organisationen avgränsar uppföljningsarbetet till att inkludera enbart kvantitativa mätetal[24]. Att kombinera dem båda ger ytterligare kvalitet i uppföljningsarbetet. Uppföljning av aktiviteter kan vara svårt för organisationer som har outsourcat driften av IT-miljön om möjlighet och upplägg för detta inte har avtalats i förväg. Detta tydliggör behovet av att dessa överväganden bör analyseras redan i ett tidigt skede under upphandlingsprocessen då olika vägval ofta får stora följdeffekter. I de fall IT-miljön är outsourcad bör även insikten om eventuella underleverantörer beaktas, det vill säga vilka tjänster som får kontrakteras till en underleverantör samt i vilken utsträckning. Hur kvaliteten i dessa tjänster ska säkerställas och vem som bär ansvaret när något fallerar är viktiga frågeställningar att beakta.

---

[20] *Faktiska utgifter som är inblandade i leveransen av tjänsten.*

[21] *Individuellt betingade utgifter som ej kan mätas i faktiska utgifter, exempelvis tid, ansträngning och interpersonella effekter.*

[22] *SOC - Security Operations Center.*

[23] *Exempel kan vara periodicitet i genomförda riskanalyser eller tredjepartsgranskningar, minskad riskexponering till följd av aktivt riskarbete, genomförda åtgärder upptäckta under övning och test, lärdomar till följd av allvarliga incidenter, trend inom kundnöjdhetsundersökningar, etc.*

[24] *Exempel kan vara uppfyllandegrad av RTO och RPO, antal återställningsplaner i förhållande till antal kritiska system, antal återställningsplaner som täcker kritiska processer, förfluten tid sedan återställningsplaner senast uppdaterades, skillnaden mellan förväntad och faktisk RTO och RPO, etc.*

Baserat på den strategiska inriktningen för styrning och kontroll bör faktiska uppföljningsaktiviteter konkretiseras på taktisk nivå. Organisationens prioriterade förmågor inom IT-kontinuitet och DR avgör vilka aktiviteter för styrning och kontroll som är mest lämpliga, varför valet av aktiviteter bör utgå ifrån de som bidrar mest till utvecklad och förbättrad förmåga. Beslut om uppföljningsaktiviteter bör baseras på fastställd ambitionsnivå samt val av kvalitativ eller kvantitativ uppföljning, eller en kombination av båda. Vidare påverkar även i vilken utsträckning som olika förmågor har outsourcats till en leverantör. Vid outsourcade drifts- och DR-tjänster är det av största vikt att tidigt involvera leverantören kring vilka aktiviteter som ska följas upp, hur ofta, samt i vilka forum som dessa uppföljningsaktiviteter ska hanteras. Det är viktigt att leverantören involveras vid lärandet och förbättringsåtgärder efter inträffade haverier. Därför bör uppföljningsaktiviteter väljas baserat på dessa ändamål. Det är också viktigt att aktiviteter följs upp på samtliga nivåer inom organisationen, det vill säga på strategisk, taktisk och operativ nivå, och att dessa hanteras inom ramen för leverantörsavtalet.

Genom god styrning och kontroll ökar möjligheten till att informationens skyddsvärden kan bibehållas genom hela DR-processen. Utmaningen för en aktör ligger ofta i att kunna bevara informationens samtliga skyddsvärden (konfidentialitet, riktighet och tillgänglighet) genom hela processen. Det finns många fallgropar under processen, men också många möjligheter. En typisk fallgrop kopplat till återställning av information gäller förvaring av och åtkomst till backupmedia. Vid en återställning måste samtliga skyddsvärden bevaras under hela hanteringen av backupmedia. Exempel på viktiga frågeställningar för en aktör är vilka personer som har rätt att hämta backupmedia, huruvida den alltid är tillgänglig, hur backupmedia ska transporteras på ett säkert sätt, hur man säkerställer att informationen lagrad på backupmedia har rätt version och är verifierad, etc. Detta behöver hanteras genom tydliga kravställningar, genom att involvera leverantörer så tidigt som möjligt under upphandlingsprocessen, genom kvalitativa strategier och planer för återställning, genom god styrning och kontroll, och slutligen genom övning och test. Samtliga av dessa åtgärder gäller oavsett om organisationen har insourcat eller outsourcat driften av sin IT-miljö.

## 2.3 *Hur utvecklas och verifieras förmågan att skydda information genom övning och test?*

### Bakgrund

Enbart genom övning och test kan den organisatoriska kontinuitetsförmågan upprätthållas och förbättras över tid. Upplägg och genomförande av dessa aktiviteter kräver noggrann planering och bör anpassas efter organisationens mål och syfte med test och övning samt dess ambitionsnivå. Ytterligare viktiga parametrar som styr planering av aktiviteter kopplade till övning och test är val av testtyp, intervall för hur ofta övningar och tester ska genomföras, samt dess komplexitet. Även den egna organisationens mognadsnivå i kombination med den fastställda övnings- och teststrategin styr hela övnings- och testverksamheten som i slutändan påverkar organisationens förmåga att möta och hantera framtida oförutsedda händelser.

Detta strategiska övervägande fokuserar på frågeställningar relaterade till övning och test ur ett förmågehöjande perspektiv. Till grund för detta ligger *Appendix K – Test av kontinuitetsplaner* i *FSPOS Vägledning för kontinuitetshantering* som tar höjd för hur tester kan planeras, genomföras och utvärderas, och som dessutom tydligt visar hur verksamhetens och IT-organisationens kontinuitetsarbete hänger samman[25]. Typexempel på frågeställningar inom detta område är sådana som berör strategi, planering, resursallokering och önskad förmåga. För aktörer i den finansiella sektorn kan avbrott i IT-tjänster få stora konsekvenser för hela verksamheten. Av denna anledning bör stort fokus läggas på dessa frågeställningar då de utgör en grundläggande förutsättning för att stärka organisationens förmåga att återställa kritisk IT-verksamhet.

### Underliggande IT-strategiska överväganden

***Strategisk nivå - Affärsstrategiska beslut för styrelsen eller ledningen som sätter ramarna***

Underliggande IT-strategiska överväganden som analyseras i detta avsnitt är:

- *Vilken ambitionsnivå och strategi gäller för övning och test?*
- *Vad är budget för övning och test och vad ska täckas in?*
- *Vad är övergripande syfte och mål med övning och test?*
- *Vem är ansvarig för planering, utförande och uppföljning av övning och test?*
- *Vilka DR-strategier bör utformas och vad bör de innehålla?*
- *Vilka förebyggande DR-aktiviteter ska täckas av IT-budgeten?*

[25] *FSPOS Vägledning för kontinuitetshantering, Appendix K – Test av kontinuitetsplaner, avsnittet för Test av IT-verksamhetens återställningsplaner.*

Som vid övriga centrala överväganden bör ambitionsnivån tydligt konkretiseras då den styr samtliga underliggande strategiska överväganden inom ramen för övning och test. Val av ambitionsnivå för övning och test bör beslutas av personer med mandat att påverka budget som ett resultat av vad som har beslutats på strategisk nivå. Detta IT-strategiska övervägande är således ett beslut som måste underbyggas med väl genomtänkta argument. IT-verksamhetens ambition för övning och test, som bör konkretiseras genom en övergripande och långsiktig övnings- och teststrategi, ska beakta kostnader, behov av resurser samt risker kopplade till övning och test. Den framtagna övnings- och teststrategin bör även inkludera en beskrivning över hur planerade övningar och tester ska bidraga till organisationens förmågeutveckling. Strategin bör även betona vikten av att öva och testa ofta och regelbundet, gärna tillsammans med övriga verksamheten, samt utnyttja redan avtalade möjligheter till övning och test tillsammans med leverantörer.

Genomförda övningar och tester resulterar ofta i behov av att revidera gällande dokument för IT-kontinuitet och DR. Det är också troligt att nya risker uppdagas gällande den tekniska lösningen som kräver omdesign av antingen enskilda IT-system eller hela återställningsmiljön om riskerna inte kan accepteras. Att hantera dessa risker är ofta förknippat med stora investeringar, både kostnadsmässigt och tidsmässigt, varför beslut om dessa måste ske strategisk nivå. De personer som beslutar om ambition, strategi och budget måste känna till, och ta höjd för, de aktiviteter som direkt och indirekt är kopplade till de faktiska övningarna och testerna då de kan leda till upptäckt av nya risker. Därför är det viktigt att besluta hur kostnader förknippade med övning och test förhåller sig till givna budgetramar samt vilka delar av organisationen som bör stå för kostnaden. Olika alternativ finns till hands, till exempel kan IT bekosta övning och test ur egen budget eller låta verksamheten stå för hela eller delar av kostnaden. Ofta är det fördelaktigt om IT och verksamheten delar på kostnaden då övnings- och testverksamheten är något som gynnar båda parter och bör därför ske i samverkan. Om IT ska bekosta sin egen övnings- och testverksamhet bör det övervägas om den ska rymmas inom befintlig IT-budget eller om extra medel behöver skjutas till.

Organisationens övergripande syfte och mål med övning och test kan även konkretiseras och förankras på strategisk nivå i den övergripande och långsiktiga övnings- och teststrategin. IT-kontinuitet och DR-hantering bör ha som huvudsyfte att skydda organisationens intressenter, rykte, varumärke och värdeskapande aktiviteter. Huvudmålet bör därför vara att genom övning och test verifiera förmågan att upprätthålla och förbättra organisationens skydd av intressenter, rykte, varumärke och värdeskapande aktiviteter över tid. Baserat på den övergripande och långsiktiga övnings- och teststrategin bör en mer specifik testplan tas fram på taktisk nivå. Viktigt att beakta i detta sammanhang är att samtliga beståndsdelar i kontinuitets- och återställningsplaner bör övas och testas, samt att detta görs tillsammans med samtliga inblandade, det vill säga verksamheten, IT och dess leverantörer. Detta bör även avspeglas i den övergripande och långsiktiga övnings- och teststrategin. I samband med att övnings- och teststrategin fastställas bör även en testorganisation utses med

fördefinierade roller och ansvar. Se vidare *Appendix K – Test av kontinuitetsplaner* i *FSPOS Vägledning för kontinuitetshantering* för fler detaljer.

Vid utformningen av DR-strategier bör verksamhetens kravställningar på bland annat *mål för återställningstid* och *mål för återhämtningspunkt* kopplat till IT-resurser[26] beaktas efter genomförd konsekvensanalys. Den beslutade DR-strategin bör således vara tätt sammanflätad med verksamhetens kontinuitetsstrategi. Till grund för utformningen av DR-strategier hänvisas till ISO 27031 som stipulerar att "*Strategies should define the approaches to implement the required resilience so that the principles of incident prevention, detection, response, recovery and restoration are put in place*". En DR-strategi bör åtminstone innehålla formulerade strategier, på IT-resursnivå, för hur avbrott ska förhindras, hur avbrott ska besvaras, samt hur IT-resursen ska återställas efter ett avbrott baserat på IT-resursens *mål för återställningstid*, *mål för återhämtningspunkt* och identifierade hot. Dessa strategier bör ta hänsyn till parametrar som budget, organisationens riskaptit, tillgängliga resurser, tekniska och andra organisatoriska begränsningar, samt regulatoriska krav. Andra faktorer som inverkar på utformningen av DR-strategin är kompetens, fysiska lokaler, tillgänglig teknologi, hur information har klassificerats, policys och processer, samt i vilken utsträckning som IT-driften har outsourcats. Den slutliga utformningen av DR-strategin kompletterar kontinuitetsstrategin för IT-verksamheten som beskrivs i *Appendix F – Kontinuitetshantering för IT-verksamheten* i *FSPOS Vägledning för kontinuitetshantering*.

***Taktisk nivå - IT-miljöstrategiska beslut för IT-ledning som beslutar om val av design, kravställning och förmågor***

Underliggande IT-strategiska överväganden som analyseras i detta avsnitt är:

- *Hur ofta ska DR-hantering och lösningar övas och med vilket syfte och mål?*
- *Hur kan leverantör involveras i test och övning för att uppnå bästa resultat?*
- *Hur och på vilka grunder planeras framtida övningsinsatser på kort och lång sikt?*
- *Hur planeras och genomförs test och övning?*
- *Hur mäts och följs resultatet av test och övning upp?*
- *Vad är syftet med och hur ska en återställningsplan användas?*
- *Ska återställningsplaner skrivas för enskilda system eller tjänster, eller vara gemensam för flera system eller tjänster?*
- *Vilka kriterier aktiverar återställningsplan?*

Med utgångspunkt från den övergripande och långsiktiga övnings- och teststrategin bör konkreta övnings- och testaktiviteter beslutas i en övnings- och testplan. Beroende på vilken ambitionsnivå som har beslutats i strategin kan övnings- och testaktiviteter planeras på kort eller lång sikt. Viktigt att överväga är vilka aktiviteter som ska genomföras, testtyp, omfattning och frekvens. Testplanen bör förslagsvis dokumentera

[26] *Alla IT-relaterade tillgångar, personer, färdigheter, teknik (innefattande anläggning och utrustning), lokaler, förråd och information (elektronisk och annan) som en organisation vid behov ska ha tillgänglig för sin verksamhet och för att nå sina mål. (ISO 22301)*

bland annat testformat, förmågeområden, prioritering, målgrupp etc. Se vidare *Appendix K – Test av kontinuitetsplaner* i *FSPOS Vägledning för kontinuitetshantering* för fler detaljer. Vid helt eller delvis outsourcad IT-miljö är det av största vikt att i ett tidigt stadium involvera leverantörer vid planering av övnings- och testaktiviteter. Ju tidigare en leverantör involveras under planeringsstadiet desto större är möjligheten till ett lyckat testresultat. Som tidigare nämnts bör redan avtalade möjligheter till övning och test tillsammans med leverantörer utnyttjas i möjligaste mån. Detta skapar även en solid grund och förutsättningar för ett större engagemang från leverantören vid framtida övnings- och testaktiviteter.

Utifrån de beslutade aktiviteterna för övning och test bör mål och mätpunkter formuleras. Exempel på parametrar som styr målsättning och val av mätpunkter är budget, tillgängliga resurser och inte minst risker kopplade till verksamheten. Ambitiösa övningar och tester riskerar att ta både tid och resurser i anspråk hos verksamheten och generera nya risker kopplade till övningen eller testet som sådant. Kopplat till planerade övnings- och testaktiviteter bör organisationen fundera över vilken dokumentation och rutiner (kontinuitetsplan, återställningsplan, beredskapsplan, etc.) som ska övas och testas respektive som ska användas som underlag vid övning och test. Detta är viktigt att överväga på taktisk nivå då det dels påverkar upplägg och planering för övning och test, dels vad som ska mätas och hur.

En återställningsplan har till uppgift att skapa en beredskap och förmåga att hantera oönskade händelser. I återställningsplanen beskrivs konkreta och tydliga kontinuitetslösningar i form av reserv-, återställnings- och återgångsrutiner för var och en av de identifierade kritiska IT-resurserna[27]. Viktiga överväganden som bör beslutas på taktisk nivå är återställningsplanernas utformning, ambitionsnivå, täckningsförmåga och grad av teknisk nivå. Dessa överväganden påverkar hur, och i vilken grad, återställningsplanerna kan användas i den operationella driften av IT-miljön. Även frågeställningen huruvida återställningsplaner ska skrivas för enskilda system eller tjänster, eller vara gemensam för flera system eller tjänster, är ett viktigt taktiskt övervägande. Genom att gruppera flera system eller tjänster i samma återställningsplan kan DR-arbetet effektiviseras och standardiserade rutiner utvecklas för system eller tjänster som delar teknisk plattform/leverantör eller stödjer samma verksamhetsprocess. På taktisk nivå behöver även kriterier för aktivering av återställningsplan beslutas, det vill säga vilka tröskelvärden som ska användas vid beslut om övergång till alternativa rutiner och initiering av återställning. Detta påverkar även utformningen av övningar och tester då tröskelvärden kan behövas överskridas för att aktivera planer.

[27] *FSPOS Vägledning för kontinuitetshantering, Appendix F – Kontinuitetshantering för IT-verksamheten, Version 3.0, Sid. 12*

# 3 Andra viktiga IT-strategiska överväganden

Detta kapitel tar upp några andra viktiga IT-strategiska överväganden som har berörts tidigare men som inte faller in under någon av de centrala IT-strategiska överväganden från föregående kapitel. De överväganden som tas upp i detta kapitel är i huvudsak frågeställningar som behöver hanteras på strategisk nivå. Dessa är:

- *Hur ska organisationer förhålla sig till Finansinspektionens föreskrifter och tillsyn?*
- *Hur kan leverantörer integreras i revisionen och tillsynen av kontinuitetsarbetet?*

*Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut* (FFFS 2014:1), *Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker* (FFFS 2014:4), samt *Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, IT-verksamhet och insättningssystem* (FFFS 2014:5), ställer höga krav på aktörer inom den finansiella sektorn. Ansvaret för att uppfylla dessa föreskrifter ligger hos den egna organisationen oavsett om man har helt eller delvis outsourcad IT-miljö. Finansiella aktörer bör göra en tydlig riskbedömning baserad på IT-strategiska överväganden och noga följa gällande föreskrifter och allmänna råd. Ett annat råd är att noga och kontinuerligt följa Finansinspektionens utgivna tillsynsrapporter som är en del i Finansinspektionens kommunikation. Rapporterna behandlar genomförda temaundersökningar och annan tillsyn som Finansinspektionen utför. Genom rapporterna informeras aktörer om vilka iakttagelser som har gjorts och om förväntningar i olika frågor. En tillsynsrapport som är av särskilt intresse inom området för IT-kontinuitet och DR är den om *Bankernas arbete med information och cybersäkerhet, Nr 9, 7 december 2018*.

För aktörer inom den finansiella sektorn är det särskilt viktigt att ha väl utvecklade och etablerade processer för hantering av risk, IT-kontinuitet, DR och compliance samt att dessa processer interagerar med varandra. Det är av största vikt att aktörer har en styrning och kontroll på samtliga nivåer inom organisationen, det vill säga på strategisk, taktisk och operativ nivå. Det är också viktigt att arbeta i rätt ordning där riskarbetet styr vilka åtgärder som behöver vidtas och prioriteras för att uppnå balans mellan tillgängliga resurser och kostnader baserat på organisationens definierade riskaptit. Dessa åtgärder innebär kravställningar inom IT-kontinuitet och DR som förväntas uppfyllas av IT-organisationen. Genom styrning och kontroll uppnås compliance gentemot de lagkrav, regleringar, policys och andra verksamhetskrav som organisationen förväntas följa. På så sätt uppnås fungerande processer som uppfyller Finansinspektionens krav inom styrning, riskhantering och kontroll.

# 4 Avslutande reflektioner

Människorna som arbetar i och för en organisation är mycket viktiga för att upprätthålla en god förmåga att hantera kontinuitets- och DR-relaterade risker. Organisationen bör därför arbeta långsiktigt och målgruppsanpassat med att höja individernas kunskap genom ett systematiskt och strukturerat kontinuitets- och DR-arbete. Arbetet bör vara förankrat på högsta ledningsnivå i organisationen och nå ut till alla anställda så att organisationens förmåga att hantera dessa risker kan upprätthållas och därigenom uppnå robusthet på en hög nivå i organisationen över tid.

Förekomsten av outsourcing inom den finansiella sektorn medför risker ur ett verksamhetsperspektiv men öppnar samtidigt upp för nya möjligheter till strategisk positionering, kostnadsbesparingar och riskhantering. Genom en noggrann analys av olika IT-strategiska överväganden kan en organisation uppnå både fler konkurrensfördelar och högre robusthet till en lägre kostnad, och därigenom frigöra resurser som kan användas till att bygga nya värdeskapande tjänster och produkter.

I framtiden kommer ännu fler faktorer att få en avgörande betydelse i takt med den IT-tekniska utvecklingen. Ett exempel är miljömässiga överväganden som kommer att få en stor påverkan på IT-strategiska beslut. Även nya arbetssätt och tekniska plattformar kommer att påverka organisationens IT-strategiska överväganden framöver. Ett sådant exempel är *DevOps*[28] som har förändrat många organisationers sätt att arbeta på, även bland aktörer inom den finansiella sektorn. Framtidens IT-användare kommer att vara mer mobil och uppkopplad, och enheter byts ut efter användarens behov. Kraven på tillgänglighet till infrastrukturen kommer att fortsätta öka, och nya tjänster och tekniska innovationer kommer att ändra förutsättningarna för att bygga robust och kostnadseffektiv disaster recovery.

[28] *DevOps härstammar från orden "development" och "operations" och är ett sätt att utveckla mjukvara eller system där ett team utvecklar, driftar, testar, integrerar och övervakar ett system i ett automatiserat flöde, vilket i praktiken innebär att teamet tar ansvar för mjukvarans eller systemets hela livscykelhantering.*

# Bilaga A. Centrala och underliggande IT-strategiska överväganden

| **Centralt IT-strategiskt övervägande** | Strategiskt underliggande överväganden | Taktiskt underliggande överväganden |
|---|---|---|
| Hur ska information hanteras utifrån hur den har klassificerats enligt organisationens beslutade kriteriemodell? | • *Kan information helt, delvis eller inte alls lagras i outsourcad IT-miljö?*<br>• *Kan information helt, delvis eller inte alls lagras i molnet?*<br>• *Finns någon information som måste lagras i egen IT-miljö?*<br>• *Finns tillräcklig kompetens internt för att drifta egen IT-miljö?*<br>• *Hur förhåller sig organisationens riskaptit till val av sourcing?*<br>• *Är det möjligt att lagra information utanför Sveriges gränser?*<br>• *Vad blir konsekvenserna av att lagra information utanför Sveriges gränser?* | • *Kan information helt, delvis eller inte alls lagras i outsourcad IT-miljö?*<br>• *Kan information helt, delvis eller inte alls lagras i molnet?*<br>• *Finns någon information som måste lagras i egen IT-miljö?*<br>• *Finns tillräcklig kompetens internt för att drifta egen IT-miljö?*<br>• *Hur förhåller sig organisationens riskaptit till val av sourcing?*<br>• *Är det möjligt att lagra information utanför Sveriges gränser?*<br>• *Vad blir konsekvenserna av att lagra information utanför Sveriges gränser?* |
| Hur säkerställs, genom styrning och kontroll, att information hanteras korrekt enligt hur den har klassificerats? | • *Hur prioriterat är systemtillgänglighet?*<br>• *I vilken utsträckning, och hur bör IT-kontinuitet och DR beaktas vid due diligence och författande av outsourcingavtal?*<br>• *Vad är ambitionsnivån och syftet med styrning och kontroll?*<br>• *Ska den huvudsakliga DR-förmågan byggas genom köpta tjänster eller interna processer och system?*<br>• *Bör DR-förmågan kvalificeras genom certifiering och i sådana fall mot vilken standard?*<br>• *Vilka lagar ska en leverantör följa om leverantören inte är registrerad i Sverige?* | • *Vad är budget vid outsourcad IT-miljö och vad ska täckas in?*<br>• *Ska uppföljning fokusera på kvalitativ eller kvantitativ information?*<br>• *Vilka DR-förmågor kan överlåtas till leverantör och vilka måste alltid finnas internt?*<br>• *I vilken omfattning får en eventuell leverantör anlita underleverantörer?*<br>• *Hur ska IT-kontinuitets- och DR-arbetet följas upp för att säkerställa önskad effekt?*<br>• *Hur kan leverantörer involveras vid lärandet och förbättringsåtgärder efter inträffade haverier?*<br>• *Hur säkerställs att informationens skyddsvärden bibehålls under hela DR-processen?* |

| **Centralt IT-strategiskt övervägande** | Strategiskt underliggande överväganden | Taktiskt underliggande överväganden |
|---|---|---|
| Hur utvecklas och verifieras förmågan att skydda information genom övning och test? | • *Vilken ambitionsnivå och strategi gäller för övning och test?*<br>• *Vad är budget för övning och test och vad ska täckas in?*<br>• *Vad är övergripande syfte och mål med övning och test?*<br>• *Vem är ansvarig för planering, utförande och uppföljning av övning och test?*<br>• *Vilka DR-strategier bör utformas och vad bör de innehålla?*<br>• *Vilka förebyggande DR-aktiviteter ska täckas av IT-budgeten?* | • *Hur ofta ska DR-hantering och lösningar övas och med vilket syfte och mål?*<br>• *Hur kan leverantör involveras i test och övning för att uppnå bästa resultat?*<br>• *Hur och på vilka grunder planeras framtida övningsinsatser på kort och lång sikt?*<br>• *Hur planeras och genomförs test och övning?*<br>• *Hur mäts och följs resultatet av test och övning upp?*<br>• *Vad är syftet med och hur ska en återställningsplan användas?*<br>• *Ska återställningsplaner skrivas för enskilda system eller tjänster, eller vara gemensam för flera system eller tjänster?*<br>• *Vilka kriterier aktiverar återställningsplan?* |

# Bilaga B. Referenslista

**Lagar och förordningar**

- Solvens II
- Basel II
- Basel III
- GDPR
- PCI DSS
- Cloud Act

**Finansinspektionens föreskrifter**

- FFFS 2014:1 – Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut
- FFFS 2014:4 – Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker
- FFFS 2014:5 – Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, IT-verksamhet och insättningssystem

**Vägledningar och metodstöd**

- Appendix F – Kontinuitetshantering för IT-verksamheten, FSPOS Vägledning för kontinuitetshantering
- Appendix G – Kontinuitetshantering för outsourcad verksamhet, FSPOS Vägledning för kontinuitetshantering
- Appendix H – Självskattningsformulär, FSPOS Vägledning för kontinuitetshantering
- Appendix K – Test av kontinuitetsplaner, FSPOS Vägledning för kontinuitetshantering
- EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02
- EBA Guidelines on ICT and security risk management, EBA/GL/2019/04
- Vägledning för fysisk informationssäkerhet i IT-utrymmen, MSB 2013
- Vägledning för identifiering av samhällsviktig verksamhet, MSB 2019
- www.informationssakerhet.se/metodstodet/utforma/#klassningsmodell

**Internationella standarder**

- ISO 9001
- ISO 14001

- ISO 27001
- ISO 22301
- ISO 27031
- ITIL 4
- COBIT 2019
- BICSI
- ANSI/TIA-942
- Uptime Institute

**Övrigt**


- FI-tillsyn – Styrning och kontroll av IT-verksamheten i försäkringsföretag, Nr 8, 15 november 2018
- FI-tillsyn – Bankernas arbete med information och cybersäkerhet, Nr 9, 7 december 2018
- Säkerhet vid molnlösningar, MSB 2018
- Terminologi och begrepp inom informationssäkerhet, MSB 2016
- The DAM Book: Digital Asset Management for Photographers, Peter Krogh 2005
- www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-plan/it-service-continuity-plan